UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,297	11/14/2003	Tong-Ming Lee	15436.188	1133

22913 7590 11/13/2007

WORKMAN NYDEGGER
60 EAST SOUTH TEMPLE
1000 EAGLE GATE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
11/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,297	LEE ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9 and 11-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9 and 11-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *22 August 2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claim 10 has been cancelled.

2. Claims 1,6,8,15,25, 28,34, and 39 have been amended.

3. Claims 1-9 and 11-41 are pending.

Information Disclosure Statement

4. The Information Disclosure Statements respectfully submitted on 22 August 2007 has been considered by the Examiner.

Response to Arguments

5. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection, Fontana et al. (Pub No. 2003/0120605).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-9 and 11-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nyman et al. (Pub No. 2003/0037033) in view of Fontana et al. (Pub No. 2003/0120605).

Referring to the rejection of claims 1 and 25, Nyman et al. discloses a network analyzer for use in a computer network having wireless components providing

encrypted data transmission and having at least two wireless access points with different encryption keysets, said network analyzer comprising:

at least one wireless card adapted to receive encrypted data on one or more channels that said at least two wireless access points are using; (See page 8, Section 0088)

and a single keyset profile stored in a data store, said single keyset profile having a plurality of encryption keysets, each encryption keyset being used to decrypt encrypted data received from a different access point of said at least two wireless access points (See page 8, Section 0094)

However, Nyman et al. does not explicitly disclose a plurality of encryption keysets.

Fontana et al. discloses a system and method for preventing unauthorized use of protected software utilizing a portable security device.

Fontana et al. discloses an analyzer adapted to decrypt said encrypted data received by said at least wireless card by using each of said plurality of encryption keysets in sequence until all of said encrypted data has been decrypted (See page 3, Sections 0036-0037)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization

process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 2 and 26, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said encrypted data is stored in non-volatile memory before said data is decrypted (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 3 and 31, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein each access point of said at least two access points utilizes a unique keyset, wherein said profile contains each unique keyset (See page 19, Section 0185)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 4 and 32, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said single keyset profile comprises a plurality of encryption keysets with each encryption keyset comprising at least two keys (See page 19, Section 0188)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 5 and 33, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein each of said access points operates on a different AP channel (See page 9, Section 0101)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 6 and 34, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said at least one wireless card receives

encrypted data from each of said access point channels for a predefined period of time (See page 9, Section 0097)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 7 and 30, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said at least one wireless card alternately receives encrypted data from each of said access points until said at least one wireless card receives a defined quantity of encrypted data from each of said access points (See page 8, Section 0088)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 8, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said data store is non-volatile memory (See page 15, Section 0152)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 9 and 27, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said encrypted data is stored in a data buffer before being stored in said data store (See page 15, Section 0153)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 11 and 37, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein each of said keysets uses at least 64 bit encryption (See page 19, Section 0187)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization

process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 12 and 38, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein each of said keysets uses at least 128 bit encryption (See page 19, Section 0187)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 13 and 40, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said profile is stored internally in the network analyzer (See page 19, Section 0191)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claims 14 and 41, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said profile is encrypted (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 15, (Nyman et al. modified by Fontana et al.) discloses in a computer network having wireless components providing encrypted data transmission and receipt and comprising at least two wireless access points, said network having a different encryption keyset for each of said at least two access points, said computer network further comprising at least one computer being connected to said network by a wireless network card and having an analyzer module, a method for decrypting data captured by said wireless network card from at least one of said at least two access points, said method comprising:

a step for establishing a keyset profile accessible by the analyzer module, said keyset profile having all keysets being used by any of said at least two access points; (See page 8, Section 0094)

a step for receiving encrypted data from at least one of said at least two access points and saving said encrypted data to a data store; (See page 8, Section 0094)

and a step for decrypting said data in said data store using said keyset profile, (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 16, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said step for saving said encrypted data further includes a step of saving said encrypted data to a data buffer before saving said data in said data store (See page 15, Section 0153)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 17, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein comprising a step for analyzing said decrypted data to identify any encrypted data (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 18, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein the step for decrypting said data includes decrypting said data using a first keyset associated with said keyset profile and decrypting said encrypted data using a second keyset associated with said keyset profile (See Fontana et al., page 3, Section 0036)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 19, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein comprising a step for repeatedly analyzing and decrypting said encrypted data until said encrypted data is completely decrypted (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 20, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said step for repeatedly analyzing and decrypting is performed without input from a user of said analyzer module (See page 8, Section 0093)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 21, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein comprising a step for selecting said keyset profile for said at least two wireless access points (See page, 18, Section 0184)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a

more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 22, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein comprising a step for accessing said keyset profile at a location of said computer network remote from said analyzer module (See page 5, Section 0041)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 23, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said keyset profile is stored in an encrypted form and further comprising a step for decrypting said keyset profile and storing a decrypted version of said keyset profile local to said analyzer module (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization

process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 24, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein comprising a step for displaying said decrypted data through at least one user interface (See page 8, Section 0093)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Referring to the rejection of claim 28, (Nyman et al. modified by Fontana et al.) discloses the claimed limitation wherein said encrypted data in said data buffer is written to said data store prior to being decrypted (See page 8, Section 0094)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Nyman et al.'s wireless system with Fontana et al.'s software prevention method. Motivation for such an implementation would enable a more secure method of authorization which makes it difficult to bypass the authorization process or create substitute authorization devices which can be used either on a host processor or on an attached co-processor (See Fontana et al., page 1, Section 0007)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
November 9, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER